

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-311083

(43)Date of publication of application : 07.11.2000

(51)Int.Cl.

G06F 9/06

(21)Application number : 11-121200

(71)Applicant : CASIO COMPUT CO LTD

(22)Date of filing : 28.04.1999

(72)Inventor : MORIKAWA SHIGENORI

IGUCHI TOSHIYUKI

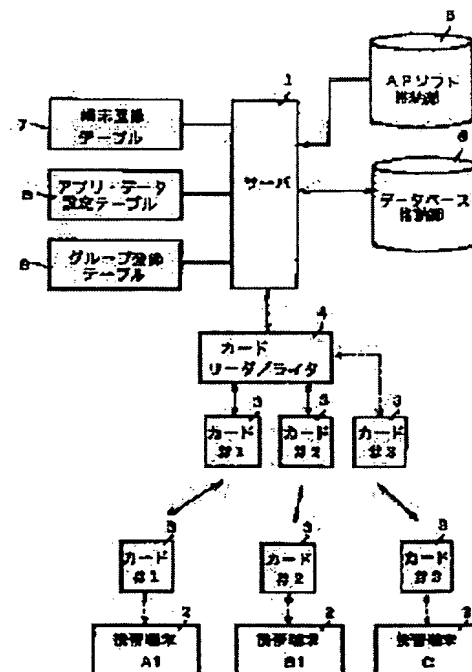
OTSUKA MOTOI

(54) PORTABLE TERMINAL EQUIPMENT, DATA DISTRIBUTING DEVICE AND METHOD AND SYSTEM FOR ACCESSING DATA

(57)Abstract:

PROBLEM TO BE SOLVED: To effectively prohibit illegal copying by means of another device which is not provided with security preservation and access authority by permitting access to application software/data in a recording medium only against a specified data processor and controlling access at every device in a data processor by which the recording medium storing application software/data is accessed to process data.

SOLUTION: In a portable terminal 2, data is processed by performing access to an AP(application) software/database in a CF card (compact flash) 3 in a state where the CF card 3 is set, where the AP software/database is stored and which is freely portable. The terminal 2 reads terminal ID which is previously stored in the CF card 3. Then terminal ID in the CF card 3 is compared with previously set one's own terminal ID and access propriety concerning the AP software/database in the CF card 3 is decided based on the comparison result.



## LEGAL STATUS

[Date of request for examination]

01.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3463239

[Date of registration]

22.08.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

- (19)【発行国】日本国特許庁(JP)  
(12)【公報種別】公開特許公報(A)  
5 (11)【公開番号】特開2000-311083(P2000-311083A)  
(43)【公開日】平成12年11月7日(2000. 11. 7)  
(54)【発明の名称】携帯端末装置、データ配布装置、データアクセス方法、及びデータアクセスシステム  
10 (51)【国際特許分類第7版】  
G06F 9/06 550  
【F1】  
G06F 9/06 550 H  
【審査請求】有  
15 【請求項の数】10  
【出願形態】OL  
【全頁数】19  
(21)【出願番号】特願平11-121200  
(22)【出願日】平成11年4月28日(1999. 4. 28)  
20 (71)【出願人】  
【識別番号】000001443  
【氏名又は名称】カシオ計算機株式会社  
【住所又は居所】東京都渋谷区本町1丁目6番2号  
(72)【発明者】  
25 【氏名】森川 重則  
【住所又は居所】東京都羽村市栄町3丁目2番1号 カシオ計算機株式会社羽村技術センター内  
(72)【発明者】  
【氏名】井口 敏之  
30 【住所又は居所】東京都羽村市栄町3丁目2番1号 カシオ計算機株式会社羽村技術センター内  
(72)【発明者】  
【氏名】大塚 基  
【住所又は居所】東京都羽村市栄町3丁目2番1号 カシオ計算機株式会社羽村技術センター内  
35 (74)【代理人】  
【識別番号】100074985  
【弁理士】  
【氏名又は名称】杉村 次郎  
40 【テーマコード(参考)】  
5B076  
【Fターム(参考)】  
5B076 FB06 FB10  
45  
(57)【要約】  
【課題】アプリケーションソフト／データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置  
50 において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト／データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ

維持と共にアクセスを有しない他の装置による不法なコピー複製を効果的に禁止する。

- 55 【解決手段】APソフト／データベースが格納されている持ち運び自在なCFカード3がセットされている状態で、このCFカード3内のAPソフト／データベースをアクセスしてデータ処理を行う携帯端末2において、携帯端末2はCFカード3内に予め格納されている端末IDを読み込む。そして、  
60 このCFカード3内の端末IDと予め設定されている自己の端末IDとを比較し、その比較結果に基づいてCFカード3内のAPソフト／データベースに対するアクセス可否を決定する。

65

【特許請求の範囲】

- 【請求項1】アプリケーションソフト／データが格納されている持ち運び自在な記録媒体がセットされている状態でこの  
70 記録媒体内のアプリケーションソフト／データをアクセスしてデータ処理を行うデータ処理装置において、前記記録媒体内のアプリケーションソフト／データをアクセスする際に、データ処理装置固有の識別情報がアクセス制御情報としてその記録媒体内に予め格納されている場合に、この記  
75 録媒体から前記識別情報を読み込む読込手段と、この読込手段によって読み込まれた識別情報と予め設定されている自己の識別情報とを比較する比較手段と、この比較手段による比較結果に基づいて前記記録媒体内のアプリ  
80 ケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備したことを特徴とするデータ処理装置。  
【請求項2】同一グループに属する複数台のデータ処理装置に対応してその装置固有の識別情報が複数格納されているグループ対応の記録媒体をアクセスする場合に、前  
85 記アクセス制御手段は前記記録媒体から読み込んだ複数の識別情報の中に、予め設定されている自己の識別情報が含まれているか否かに基づいて当該記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定するようにしたことを特徴とする請求項1記載のデータ処理装置。  
90 【請求項3】前記記録媒体内に複数のアプリケーションソフト／データが格納されていると共に、個々のアプリケーションソフト／データに対応付けてデータ処理装置固有の識別情報が格納されている場合に、前記読込手段はア  
95 クセス対象として指定されたアプリケーションソフト／データに対応する識別情報を読み込み、前記アクセス制御手段は前記記録媒体から読み込まれた識別情報と予め設定されている自己の識別情報とを比較することによりアプリケーションソフト／データ毎にアクセス可否を決定するようにしたことを特徴とする請求項1記載のデータ処理装置。  
【請求項4】持ち運び自在な記録媒体にアプリケーションソフト／データを書き込むことにより、この記録媒体を介して各端末側にアプリケーションソフト／データを配布するデータ処理装置において、アプリケーションソフト／データを

アクセスすることが許可／禁止された端末に対して予め割り当てられている端末固有の識別情報をアクセス制御情報として取得する取得手段と、この取得手段によって得られた端末識別情報をアプリケーションソフト／データに対応付けてその記録媒体内に書き込む書込手段とを具備したことを特徴とするデータ処理装置。

【請求項5】個々のアプリケーションソフト／データ毎にそのアクセスを許可／禁止する端末を定義する定義情報を参照し、前記書込手段は端末対応の記録媒体毎に書き込み対象としてのアプリケーションソフト／データを特定すると共に、特定されたアプリケーションソフト／データをその端末識別情報と共に記録媒体内に書き込むようにしたことを特徴とする請求項4記載のデータ処理装置。

【請求項6】同一グループに属する複数の端末へ前記記録媒体を介してアプリケーションソフト／データを配布する際に、前記取得手段は、そのグループに属する各端末固有の識別情報を複数取得し、前記書込手段はこの取得手段によって得られた同一グループに属する複数の端末識別情報をアプリケーションソフト／データと共に書き込むようにしたことを特徴とする請求項4記載のデータ処理装置。

【請求項7】端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、各アプリケーションソフト／データに対応して端末識別情報をアクセス制限情報として記憶するアクセス制限情報記憶手段と、いずれかの端末装置からアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来た端末識別情報とアプリケーションソフト／データに対応する端末識別情報とを比較する比較手段と、この比較手段による比較結果に基づいてアプリケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備したことを特徴とするデータ処理装置。

【請求項8】コンピュータによって読み取られるプログラムコードを有する記録媒体であって、アプリケーションソフト／データが格納されている持ち運び自在な記録媒体がセットされている状態での記録媒体内のアプリケーションソフト／データをアクセスする際に、この記録媒体からデータ処理装置固有の識別情報を読み込む機能と、この識別情報と予め設定されている自己の識別情報とを比較する機能と、この比較結果に基づいて前記記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定する機能を実現するためのプログラムコードを有する記録媒体。

【請求項9】コンピュータによって読み取られるプログラムコードを有する記録媒体であって、アプリケーションソフト／データをアクセスすることが許可／禁止されている端末に対して予め割り当てられている端末固有の識別情報をアクセス制御情報として取得する機能と、このアプリケーションソフト／データに対応付けてその記録媒体内に書き込む機能を実現するためのプログラムコードを有する記録媒体。

【請求項10】コンピュータによって読み取られるプログラムコードを有する記録媒体であって、いずれかの端末装置からネットワークを介してアプリケーションソフト／データ

に対するアクセス要求があった際に、要求元の端末装置から送信されて来た端末識別情報と、アプリケーションソフト／データに対応する端末識別情報とを比較する機能と、この比較結果に応じてアプリケーションソフト／データに対するアクセス可否を決定する機能を実現するためのプログラムコードを有する記録媒体。

詳細な説明

#### 【発明の詳細な説明】

#### 【0001】

【発明の属する技術分野】この発明は、アプリケーションソフト／データのアクセスを制御するデータ処理装置およびそのプログラム記録媒体に関する。

#### 【0002】

【従来の技術】一般に、アプリケーションソフトはフロッピーディスクやコンパクトディスク等の記録媒体を介してパーソナルコンピュータ（パソコン）に別途提供され、これをパソコン上でインストールすることにより起動される。この場合、ソフトメーカはアプリケーションソフトにユニークなプロダクト番号を付けて出荷する。このソフトをユーザがパソコン上でインストールして動作させる場合、許可キーとしてこのプロダクト番号をキーボードから入力するようにしている。一方、複数台の端末装置がネットワークを介して通信接続されて成るオンライン型のクライアント・サーバシステムにおいて、各クライアント端末はネットワークを経由してアプリケーションソフトを入手するようにしている。この場合、クライアント端末からサーバへアプリケーションソフトのコピー転送を要求するが、その際、ユーザは自己のIDとパスワードを入力するようにしている。

#### 【0003】

【発明が解決しようとする課題】しかしながら、記憶媒体を介して提供されるアプリケーションソフトは、そのプロダクト番号さえ分かれば、複数台のパソコンに何回もインストールすることができ、不法なコピー複製が可能となる。このようなコピー複製を禁止するためには、一旦、アプリケーションソフトをインストールしたらその記憶媒体の内容を全てクリアする必要がある。しかしながら、記憶媒体の内容を全てクリアしてしまうと、その後、障害が発生し、再度インストールする必要が生じたときには、それに対応することができなくなり、また記憶媒体の内容をその都度クリアするという面倒な作業を強要することにもなる。また、ネットワーク経由でクライアント端末からサーバへアクセスする場合、ユーザIDとパスワードとを知っていれば、誰でもどの端末からでもアプリケーションソフトをアクセスすることができ、不正アクセスの可能性がある。このことはアプリケーションソフトに限らず、機密性の高い重要データを記憶媒体を介して提供する場合やネットワーク経由で提供する場合においても同様であり、セキュリティ維持の点で問題があった。第1の発明の課題は、アプリケーションソフト／データが格納されている記録媒体をアクセス

してデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト/データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止できるようにすることである。第2の発明の課題は、アプリケーションソフト/データを記録媒体に書き込んで各端末に配布するデータ処理装置において、特定端末に対してのみアプリケーションソフト/データのアクセスを許可/禁止するための書き込みを行うことで、端末毎のアクセス制御が可能となりセキュリティ維持と共に、アクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止できるようにすることである。第3の発明の課題は、端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、特定端末に対してのみアプリケーションソフト/データのアクセスを許可することで、不法なアプリケーションソフト/データのダウンロードを禁止し、そのセキュリティを維持できるようにすることである。

#### 【0004】

【課題を解決するための手段】この発明の手段は次の通りである。請求項1記載の発明（第1の発明）は、アプリケーションソフト/データが格納されている持ち運び自在な記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト/データをアクセスしてデータ処理を行うデータ処理装置において、前記記録媒体内のアプリケーションソフト/データをアクセスする際に、データ処理装置固有の識別情報がアクセス制御情報としてその記録媒体内に予め格納されている場合に、この記録媒体から前記識別情報を読み込む読入手段と、この読入手段によって読み込まれた識別情報と予め設定されている自己の識別情報とを比較する比較手段と、この比較手段による比較結果に基づいて前記記録媒体内のアプリケーションソフト/データに対するアクセス可否を決定するアクセス制御手段とを具備するものである。なお、同一グループに属する複数台のデータ処理装置に対応してその装置固有の識別情報が複数格納されているグループ対応の記録媒体をアクセスする場合に、前記アクセス制御手段は前記記録媒体から読み込んだ複数の識別情報の中に、予め設定されている自己の識別情報が含まれているか否かに基づいて当該記録媒体内のアプリケーションソフト/データに対するアクセス可否を決定するようにしてもよい。また、前記記録媒体内に複数のアプリケーションソフト/データが格納されていると共に、個々のアプリケーションソフト/データに対応付けてデータ処理装置固有の識別情報が格納されている場合に、前記読入手段はアクセス対象として指定されたアプリケーションソフト/データに対応する識別情報を読み込み、前記アクセス制御手段は前記記録媒体から読み込まれた識別情報と予め設定されている自己の識別情報とを比較することによりアプリケーションソフト/データ毎にアクセス可否を決定するようにしてもよい。請求項1記載

の発明においては、アプリケーションソフト/データと共にデータ処理装置固有の識別情報（例えば、端末ID）が格納されている記録媒体をアクセスする際に、この記録媒体から識別情報を読み込み、この識別情報と予め設定されている自己の識別情報とを比較し、この比較結果に基づいて記録媒体内のアプリケーションソフト/データに対するアクセス可否を決定する。したがって、アプリケーションソフト/データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト/データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止することができる。

【0005】請求項4記載の発明（第2の発明）は、持ち運び自在な記録媒体にアプリケーションソフト/データを書き込むことにより、この記録媒体を介して各端末側にアプリケーションソフト/データを配布するデータ処理装置において、アプリケーションソフト/データをアクセスすることが許可/禁止された端末に対して予め割り当てられている端末固有の識別情報をアクセス制御情報として取得する取得手段と、この取得手段によって得られた端末識別情報をアプリケーションソフト/データに対応付けてその記録媒体内に書き込む書込手段とを具備するものである。なお、個々のアプリケーションソフト/データ毎にそのアクセスを許可/禁止する端末を定義する定義情報を参照し、前記書込手段は端末対応の記録媒体毎に書き込み対象としてのアプリケーションソフト/データを特定すると共に、特定されたアプリケーションソフト/データをその端末識別情報と共に記録媒体内に書き込むようにしてもよい。また、同一グループに属する複数の端末へ前記記録媒体を介してアプリケーションソフト/データを配布する際に、前記取得手段は、そのグループに属する各端末固有の識別情報を複数取得し、前記書込手段はこの取得手段によって得られた同一グループに属する複数の端末識別情報をアプリケーションソフト/データと共に書き込むようにしてもよい。請求項4記載の発明においては、アプリケーションソフト/データをアクセスすることが許可/禁止された端末に対して予め割り当てられている端末固有の識別情報を取得し、この識別情報をアプリケーションソフト/データに対応付けてその記録媒体内に書き込む。したがって、アプリケーションソフト/データを記録媒体に書き込んで各端末に配布するデータ処理装置において、特定端末に対してのみアプリケーションソフト/データのアクセスを許可/禁止するための書き込みを行うことで、端末毎のアクセス制御が可能となりセキュリティ維持と共に、アクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止することができる。

【0006】請求項7記載の発明（第3の発明）は端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、各アプリケーションソフト/デ

ータに対応して端末識別情報をアクセス制限情報として記憶するアクセス制限情報記憶手段と、いずれかの端末装置からアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来た端末識別情報とアプリケーションソフト／データに対応する端末識別情報とを比較する比較手段と、この比較手段による比較結果に基づいてアプリケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備するものである。請求項7記載の発明においては、いずれかの端末装置からアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来る端末識別情報と、アプリケーションソフト／データに対応する端末識別情報とを比較し、その比較結果に応じてアプリケーションソフト／データに対するアクセス可否を決定する。したがって、端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可することで、不法なアプリケーションソフト／データのダウンロードを禁止し、そのセキュリティを維持することができる。

#### 【0007】

【発明の実施の形態】(第1実施形態) 以下、図1～図7を参照してこの発明の第1実施形態を説明する。図1はオフライン型のクライアント・サーバシステムを示したシステム構成図である。すなわち、会社組織において、会社内に設置されているサーバコンピュータ1と、各営業担当者が持参するモバイル型のクライアント端末(携帯端末)2とを有し、各営業担当者は外出先で可搬型記録媒体3内のアプリケーションソフト／データベースをアクセスしながら営業活動を行い、そして、一日の営業終了時に、端末本体から可搬型記録媒体3を抜き取り、サーバコンピュータ1のカードリーダー／ライタ4にセットすると、サーバコンピュータ1はカードリーダー／ライタ4を介してCFカード3内の営業記録を収集処理するオフライン型のシステムである。ここで、可搬型の記録媒体3は取り外し可能なコンパクトフラッシュカードであり、以下、CFカード3と称する。サーバコンピュータ1に付属されているカードリーダー／ライタ4は、各クライアント端末対応のCFカード3が複数枚同時にセット可能なもので、各CFカード3を順次アクセスしてデータの読み込み／書き込みを行う。なお、図中、CFカード3に付した「#1」、「#2」、「#3」は、端末名称「A1」、「B1」、「C1」で示される携帯端末2に対応付けられ、携帯端末2と1:1に対応付けられた端末対応のCFカード3であることを示している。なお、この実施形態においては端末対応のCFカード3の他、後述する端末グループ対応のCFカード3も存在するが、図1の例では端末対応のCFカード3のみを示している。サーバコンピュータ1はこのCFカード3を介して携帯端末2側へアプリケーションソフト(APソフト)／データベースを配布する。すなわち、サーバコンピュータ

1はAPソフト格納部5、データベース格納部6の内容を読み出してカードリーダー／ライタ4に与え、それにセットされている各CFカード3にAPソフト／データベースを書き込むが、その際、サーバコンピュータ1は端末登録テーブル7、アプリ・データ設定テーブル8を参照してどの端末に何を書き込むかを判別し、APソフト／データベースを特定して該当するCFカード3内に書き込むと共に端末識別情報(端末ID)をAPソフト／データベースに対するアクセス制御情報としてCFカード3内に書き込む。

【0008】図2はCFカード3に格納されているデータを示したもので、(A)は端末対応のCFカード3の内容を示している。この端末対応のCFカード3は、それを識別するための固有の媒体番号と、このカードを専用する携帯端末2を識別するための固有の端末IDと、APソフト、データベースとを記憶する構成で、この例では媒体番号「M01」、端末ID「ID11」、APソフト「a1」、データベース「D1」が格納されている。ここで、APソフト／データベースと端末IDとの対応関係は、そのアクセスを許可する端末を定義するもので、端末対応のCFカード3には1種類の端末IDが設定されている。また、図2(B)は端末グループA対応のCFカード3の内容を示し、図3に示すように「#1A」を付した各CFカード3は、端末名称が「A1」、「A2」、「A3」である各携帯端末2が属する端末グループA対応の記憶媒体で、そのグループ対応の各CFカード3には、「媒体番号」の他、各種のAPソフト／データベース毎に1または2以上の端末IDが格納されており、「媒体番号」を除く他のデータは、そのグループ内において同一内容となっている。なお、図2(A)で示した端末IDは図3に示すように端末グループAに属する各携帯端末2毎に割り当てられた固有の端末識別情報であり、APソフト／データベースと端末IDとの対応関係は、端末対応の場合と同様に、そのアクセスを許可する端末を定義する。また、図2(C)は端末グループB対応のCFカード3の内容を示し、そのデータ構造は図2(B)で示した端末グループAの場合と同様であるため、その説明は省略するが、端末グループB対応の各CFカード3内に設定された端末IDは、図3に示すように端末グループBに属する各携帯端末2毎に割り当てられた端末識別情報である。

【0009】図4はサーバコンピュータ1側に設けられている端末登録テーブル7、アプリ・データ設定テーブル8、グループ登録テーブル9のデータ構造を示したもので、図4(A)は端末登録テーブル7の内容を示している。この端末登録テーブル7はアプリ・データ設定テーブル8を作成する際や端末対応のCFカード3にAPソフト／データベースを書き込む際に参照されるもので、「端末名称」、「端末ID」、「媒体番号」とを対応付けた構成で、システム構築時や新たな媒体を追加採用するとき等にその設定登録が行われる。アプリ・データ設定テーブル8は図4(B)に示すように、APソフト／デー

データベース毎に、そのソフト名／データベース名に対応付けて、1または2以上の端末IDを記憶する構成で、サーバコンピュータ1はCFカード3にAPソフト／データベースを書き込む際に参照される。

5 【0010】図5は、サーバコンピュータ1、携帯端末2の全体構成を示したブロック図である。なお、サーバコンピュータ1、携帯端末2の構成要素は基本的に同一であるため、図中11～16はサーバコンピュータ1に  
10 対応する構成要素とし、図中21～26は携帯端末2に対応する構成要素として以下、説明するものとする。CPU11(21)は各種プログラムにしたがってこのサーバコンピュータ1(携帯端末2)の全体動作を制御する中央演算処理装置である。記憶装置12(22)はオペレーティングシステムや各種アプリケーションプログラム、データベース、文字フォントデータ等が予め格納されている記憶媒体13(23)やその駆動系を有している。この記憶媒体13(23)は固定的に設けたもの、もしくは着脱自在に装着可能なものであり、フロッピーディスク、ハードディスク、光ディスク、RAMカード等の磁気的・光学的記憶媒体、半導体メモリによって構成されている。また、記憶媒体内のプログラムやデータは、必要に応じてCPU11(21)の制御により、RAM14(24)にロードされる。更に、CPU11(21)は通信回線を介して他の機器側から送信されて来たプログラム、データを受信して記憶媒体に格納したり、他の機器側に設けられている記憶媒体に格納されているプログラム、データを通信回線を介して使用することもできる。また、CPU11(21)にはその入出力周辺デバイスである入力装置15(25)、表示装置16(26)がバスラインを介して接続されており、入出力プログラムにしたがってCPU11(21)はそれらの動作を制御する。

【0011】次に、このクライアント・サーバシステムの動作を図6および図7に示すフローチャートにしたがって説明する。ここで、これらのフローチャートに記述されている各機能を実現するためのプログラムは、読み取り可能なプログラムコードの形態で記憶媒体13(23)に格納されており、CPU11(21)はこのプログラムコードにしたがった動作を逐次実行する。なお、  
40 このことは後述する他の実施形態についても同様である。図6はサーバコンピュータ1側の特徴的な動作を示したフローチャートである。まず、アプリ・データ設定テーブル8に対してその内容を任意に設定する設定登録が指示された場合には(ステップA1)、アプリ・データ設定  
45 テーブル8に設定すべきAPソフト／データベースの名称を選択すると共に、このAPソフト／データベースに対してそのアクセスを許可する携帯端末2の端末名称を選択する(ステップA3)。すると、選択されたAPソフト／データベースの名称がアプリ・データ設定テーブル  
50 8に書き込まれるときに、選択された端末名称に対応する端末IDを端末登録テーブル7から取得し、この端末IDをAPソフト／データベースの名称に対応付けてア

プリ・データ設定テーブル8に書き込む(ステップA4)。このようにして1レコード分のデータをアプリ・データ設定テーブル8に設定し終ると、設定終了が指示されたかを調べ(ステップA5)、設定終了が指示されるまで上述の動作が繰り返される(ステップA2～A4)。

【0012】次に、CFカード3への書き込みが指示された場合には(ステップA6)、カードリーダー／ライター4にCFカード3がセットされていることを条件に(ステップA7)、CFカード3への書き込み処理に移る。まず、書き込みタイプの選択を行う(ステップA8)。ここで、ユーザは端末対応のCFカード3への書き込みか、端末グループ対応のCFカード3への書き込みかを選択指定すると、選択された書き込み形式の判別が行われる。いま、端末対応の書き込みが選択指定された場合には、カードリーダー／ライター4にセットされているCFカード3から「媒体番号」を読み出し(ステップA9)、媒体番号対応の端末IDを端末登録テーブル7から取得する(ステップA10)。そして、端末IDに基づいてアプリ・データ設定テーブル8を検索し、端末ID対応のAPソフト／データベースの名称を取得し、それに応じてAPソフト格納部5、データベース格納部6から該当するAPソフト／データベースを読み出す(ステップA11)。いま、図4(B)に示すアプリ・データ設定テーブル8において、端末IDが「ID11」であれば、それに該当するAPソフトとして「α1」、データベースとして「D1」がAPソフト格納部5、データベース格納部6から読み出される。

【0013】このようにして取得した端末ID対応のAPソフト／データベースをそのCFカード3へ書き込むと共に(ステップA12)、上述のステップA10で取得した端末IDをそのAPソフト／データベースに対するアクセス制御情報として書き込む(ステップA13)。このような書き込みが終ると、その端末IDに対応してアプリ・データ設定テーブル8に書き込み済であることを示す「書き込みフラグ」をセットする(ステップA14)。そして、カードリーダー／ライター4に複数枚のCFカード3がセットされてる場合、未書き込みのCFカード3が有るかを調べ(ステップA15)、有ればステップA9に戻り、次のCFカード3をアクセスしてその「媒体番号」を読み出し、そのCFカード3に対して上述と同様の書き込み処理を行う。これによってセット中の全てのCFカード3に対してその書き込みが終ると、アプリ・データ設定テーブル8を参照し、「書き込みフラグ」がセットされていない端末IDを抽出し、この端末IDに該当する端末名称を端末登録テーブル7から取得し、未書き込み端末名称として一覧表示させると共に(ステップA16)、書き込み完了メッセージを表示出力させる(ステップA17)。

【0014】一方、端末グループ対応のCFカード3に対応する書き込みが選択指定された場合には、端末グループ名の選択画面が表示され、その中から所望のグループ名を選択指定すると(ステップA18)、このグループ

名に基づいてグループ登録テーブル9を検索し、該当する複数の端末IDを取得する(ステップA19)。そして、この複数の端末IDに基づいてアプリ・データ設定テーブル8の内容をその先頭から検索し、その端末IDが1  
5 つでも含まれていれば、それに対応するAPソフト/データベースをAPソフト格納部5、データベース格納部6から読み出す(ステップA20)。ここで、端末グループAが選択された場合には、APソフト「a1」を取得  
60 する。そして、取得したAPソフト/データベースをそれに対応する端末IDと共にCFカード3に書き込む(ステップA21、A22)。この場合、APソフト「a1」と端末ID「ID11」、「ID12」とが対応付けられてCFカード3に書き込まれる。そして、カードリーダー/ライタ4にセットされている全てのCFカード3  
15 に対して同様の書き込みが終了するまで柔術の動作が繰り返される(ステップA21~A23)。これによって全媒体への書き込みが終了すると、ステップA24に進み、同一グループ内において未書き込みのAPソフト/データベースがアプリ・データ設定テーブル8内にまだ有るかを調べ、有ればステップA20に戻るため、次に、端末グループAに該当するAPソフトとして「a2」が読み  
20 出され、端末ID「ID13」と共に各CFカード3に書き込まれる。以下、同様に、データベース「D1」、端末ID「ID11」が各CFカード3に書き込まれ、次  
25 でデータベース「D2」、端末ID「ID12」、更にデータベース「D3」、端末ID「ID13」が各CFカード3に書き込まれる。この結果、端末グループA対応の各CFカード3の内容は、図2(B)に示す如くとなり、端末グループA対応の書き込みが全て完了すると、書き込み完了メッセージが表示される(ステップA17)。このようにしてAPソフト/データベースの書き込みが行われたCFカード3は、対応する携帯端末2側へそれぞれ配布される。

【0015】図7は携帯端末2側の動作を示したフロー  
35 チャートであり、電源投入に伴って実行開始される。先ず、初期メニュー画面の中から任意のAPソフト/データベースが選択されてその起動アクセスが指示された場合に(ステップB1)、その携帯端末2にCFカード3が  
40 セットされていなければ(ステップB2)、その起動アクセスを無効とするためにステップB1に戻るが、CFカード3がセットされていれば、予め設定されている自己の端末IDを読み出す(ステップB3)。そして、CFカード3をアクセスしてそれに格納されている端末IDを  
45 読み出し(ステップB4)、自己の端末IDと一致するかを調べる(ステップB5)。この場合、グループ対応のCFカード3にはAPソフト/データベース毎にそのグループに属する他の端末IDも格納されているので、選択指定されたAPソフト/データベースに対応する端末IDをCFカード3から読み出し、その中に自己の端末ID  
50 Dが含まれているかを調べる。ここで、端末IDの一致が検出された場合にはそれを条件に選択指定されたAPソフト/データベースのアクセスが許可され、それに応

じた処理の実行に移行する(ステップB6)、端末IDの不一致が検出された場合にはステップB1に戻るため、そのAPソフト/データベースのアクセスは禁止される。

【0016】以上のようにこの第1実施形態において、CFカード3内のAPソフト/データベースをアクセスしてデータ処理を行う際に、携帯端末2はCFカード3から読み込んだ端末IDと予め設定されている自己の端末IDとを比較し、その一致/不一致によってCFカード3内のAPソフト/データベースに対するアクセスが制御されるので、特定の携帯端末2に対してのみCFカード3内のAPソフト/データベースをアクセスすることが可能となる。つまり、CFカード3内のAPソフト/データベースをアクセスすることができる携帯端末2を制限するようにしたから、端末毎のアクセス制御が可能となると共に、アクセス権限を有しない他の携帯端末2による不法なコピー複製を効果的に禁止することができる。このことは端末対応のCFカード3に限らず、グループ対応のCFカード3についても同様であり、営業地域毎に特定のAPソフト/データベースを使用する場合、地域毎に端末グループを分けておけば、端末グループ毎のアクセス制御が可能となる。またCFカード3内に個々のAPソフト/データベースに対応付けて端末IDが格納されている場合には、端末毎、APソフト/データベース毎にそのアクセス制御が可能となる。すなわち、CFカード3内に複数のAPソフト/データベースが格納されている場合、特定のAPソフト/データベースに対してはアクセスが許可されるが、他のAPソフト/データベースについてはそのアクセスを禁止することができ、同一の端末グループに属する携帯端末2であっても、APソフト/データベース毎にそのアクセスを制御することが可能となる。

【0017】一方、サーバコンピュータ1はCFカード3内のAPソフト/データベースを書き込むことによりこのCFカード3を介して携帯端末2側にAPソフト/データベースを配布するが、その際、サーバコンピュータ1はこのCFカード3に対応付けられている端末IDを読み出してCFカード3内にAPソフト/データベースと共にこの端末IDを書き込むようにしたから、APソフト/データベースのアクセスを許可する携帯端末2を特定することができる。これによって端末毎のアクセス制御が可能となると共に、アクセス権限を有しない他の携帯端末2による不法なコピー複製を効果的に禁止することができる。また、サーバコンピュータ1は個々のAPソフト/データベース毎にそのアクセスを許可する端末を定義するアプリ・データ設定テーブル8を参照することによって端末対応のCFカード3毎に、書き込み対象のAPソフト/データベースを特定することができる。このことは、端末対応のCFカード3に限らず、グループ対応のCFカード3についても同様であり、同じ端末グループに属する各携帯端末2の端末IDをCFカード3内に書き込むことで、APソフト/データベースのアクセスを許可する端末グループを特定することがで



き、これによって端末グループ毎にアクセス制御が可能となる。

【0018】なお、上述した第1実施形態は持ち運び自在な記憶媒体としてCFカードを示したが、これに限らず、磁氣的、光学的記録媒体、半導体メモリ等、任意であり、またカード型に限らず、カートリッジ型のディスク等であってもよい。また、クライアント端末はモバイル型の携帯端末2に限らず、デスクトップ型の端末であつてもよい。更に、記録媒体内のAPソフト/データベースに対応してそのアクセスを許可する端末IDを書き込む場合に限らず、そのアクセスを禁止する端末IDを書き込むようにしてもよい。

【0019】(第2実施形態) 以下、図8～図10を参照してこの発明の第2実施形態を説明する。なお、上述した第1実施形態においては、持ち運び自由な可搬型の記憶媒体を介してサーバコンピュータ1と携帯端末2との間でデータの授受を行うオフライン型のクライアント・サーバシステムを示したが、この第2実施形態は複数台のクライアント端末がネットワークを介してサーバコンピュータに通信接続されて成るオンライン型のクライアント・サーバシステムに適用したもので、基本的には第1実施形態と同様の構成となっている。

【0020】図8はこの第2実施形態におけるクライアント・サーバシステムを示したシステム構成図であり、このクライアント・サーバシステムはサーバコンピュータ31に専用回線あるいは公衆回線を介して複数台のクライアント端末32が接続されたローカルエリアネットワークあるいは広域ネットワークシステムである。このサーバコンピュータ31側には端末登録テーブル33、アプリ・データ設定テーブル34が設けられている。この端末登録テーブル33、アプリ・データ設定テーブル34は上述した第1実施形態で示した端末登録テーブル7、アプリ・データ設定テーブル8 (図4 (A)、(B) 参照) と基本的に同様の構成で、端末登録テーブル33は「端末名称」、「端末ID」とを対応付けた構成となっている。また、アプリ・データ設定テーブル34はAPソフト/データベース毎にそのアクセスを許可する端末を識別するための端末IDを対応付けて記憶するもので、各APソフト/データベースに対応付けて1または2以上の端末IDが記憶されている。ここで、クライアント端末32側からAPソフト/データベースの送信要求が有った際に、サーバコンピュータ31は端末登録テーブル33、アプリ・データ設定テーブル34を参照し、要求されたAPソフト/データベースに対してそのアクセスが許可されている端末からの要求であれば、それを条件に、APソフト/データベースを要求元へ送信するようになっている。

【0021】次に、この第2実施形態の動作を図9、図10に示すフローチャートにしたがって説明する。図9はクライアント端末32側の動作を示し、図10はサーバコンピュータ31側の動作を示したフローチャートである。先ず、クライアント端末32側において、自己の

端末IDをサーバコンピュータ31側の端末登録テーブル33に登録すべきID登録が指示された場合には(ステップC1)、自己の端末名称を入力したのち(ステップC2)、予め設定されている自己の端末IDを読み出し(ステップC3)、サーバコンピュータ31に対してID登録を要求し、OK応答(肯定応答)が有るまでID登録を要求し続ける(ステップC4、C5)。ここで、OK応答が有れば、端末IDをサーバコンピュータ31へ送信する(ステップC6) ここで、サーバコンピュータ31側においては、端末側からの要求がID登録であれば(ステップD2～D4)、その要求を正常に受信したことを示すために要求元へOK応答を返信し(ステップD16)、これによってクライアント端末32側から送信されて来る端末名称、端末IDを受信すると(ステップD17)、それが予め決められている書式通りのデータであれば(ステップD18)、端末登録テーブル33にこの端末名称と端末IDとを対応付けて登録する(ステップD19)。そして、正常登録した旨を示すために、要求元へOK応答を行う(ステップD20)。一方、端末から送信されて来た端末名称、端末IDが書式通りのデータでなければ、要求元に対してエラー応答を行う(ステップD15)。これによってクライアント端末32側ではサーバコンピュータ31からの応答がOK応答であれば(ステップC7)、登録終了メッセージを表示させるが(ステップC8)、エラー応答であればエラーメッセージを表示させる(ステップC9)。

【0022】このようにサーバコンピュータ31は各クライアント端末32からID登録が要求される毎に、端末名称、端末IDとを対応付けて端末登録テーブル33に順次登録してゆく。一方、サーバコンピュータ31側において、APソフト/データベースに対するアクセスをどの端末に許可するかをAPソフト/データベース毎に設定するために、その設定を指示すると、上述した第1実施形態と同様の処理(図6のステップA1～A5)によってアプリ・データ設定テーブル34が作成される(ステップD1、D5～D8)。このようにサーバコンピュータ31側に端末登録テーブル33、アプリ・データ設定テーブル34が作成されている状態で、クライアント端末32側でAPソフト/データベースの送信要求を指示すると(図10のステップC10)、予め設定されている自己の端末IDを読み出し(ステップC11)、サーバコンピュータ31に対してAPソフト/データベースの送信要求を行いOK応答が有るまで要求し続け(ステップC12、C13)、OK応答が有れば端末IDを送信する(ステップC14)。

【0023】一方、サーバコンピュータ31側においては、クライアント端末32からの要求がAPソフト/データベースの送信要求であれば(ステップD2、D3)、要求元へOK応答を送信したのち(ステップD9)、端末IDの受信待ちとなり、要求元からの端末IDを受信すると(ステップD10)、受信した端末IDに基づいて端末登録テーブル33を検索し、予め登録されている正規

の端末からの要求であるかを調べる（ステップD11）。ここで、正規の端末からの要求でなければ、その要求元へエラー応答を行うが（ステップD15）、正規の端末からの要求であれば、要求元へOK応答を行うと共に（ステップD12）、その端末IDに基づいてアプリ・データ設定テーブル34を検索し、端末ID対応のAPソフト／データベースを選択的に読み出して要求元へ送信する（ステップD13、D14）。この場合、端末ID対応のAPソフト／データベースが複数存在していれば、その全てを要求元へ送信するようにしてもよいが、所望のAPソフト／データベースのみの送信要求があれば、要求されたAPソフト／データベースだけを送信する。すると、クライアント端末32側においては、サーバコンピュータ31からエラー応答が有れば（ステップC15）、エラーメッセージを表示出力させるが（ステップC9）、OK応答が有れば（ステップC15）、サーバコンピュータ31側から通信されて来たAPソフト／データベースを受信して登録保存する（ステップC16、C17）。そして、このAPソフト／データベースを起動させてデータ処理を開始する（ステップC18）。なお、サーバコンピュータ31からのAPソフト／データベースが登録保存されている状態においては、その起動指示に応じていつでも自由にAPソフト／データベースにしたがったデータ処理を実行することができる（ステップC19、C18）。

【0024】以上のようにこの第2実施形態におけるオンライン型のクライアント・サーバシステムにおいては、いずれかのクライアント端末32からAPソフト／データベースに対するアクセス要求があった際に、要求元のクライアント端末32から送信されて来た端末IDと、アプリ・データ設定テーブル34内のAPソフト／データベースに対応する端末IDとを比較し、その比較結果に応じてAPソフト／データベースに対するアクセス可否を決定するようにしたから、特定端末に対してのみAPソフト／データベースのアクセスを許可することで、不法なAPソフト／データベースのダウンロードを禁止し、そのセキュリティを維持することが可能となる。

【0025】なお、上述した第2実施形態においては、端末登録テーブル33を設けたが、アプリ・データ設定テーブル34だけ設ける構成としてもよい。また、APソフト／データベースの送信要求に応じてAPソフト／データベースを要求元へ送信するようにしたが、クライアント端末32がサーバコンピュータ31内のAPソフト／データベースを直接アクセスするようにしてもよい。またオンライン型システムに限らず、無線通信や光通信を媒体とするシステムであってもよい。また、上述した各実施形態において、端末IDの構成は任意であり、端末製造時の製造番号、例えば、「国コード+製造会社コード+機能コード+端末シリアル番号」であってもよい。また公衆電話回線をネットワークとするシステムにおいては、「国電話コード+地域電話コード+電話番号」であってもよい。更に、APソフト／データベースと端末ID

Dとを対応付けたテーブルに限らず、APソフト／データベース毎にそのアクセスを許可する端末あるいはそのアクセスを禁止する端末を論理条件式で記述したテーブルとしてもよい。例えば、等号、不等号を用いて端末IDの番号が所定範囲内にあればアクセス可あるいは不可を定義するようにしてもよい。

#### 【0026】

【発明の効果】第1の発明によれば、アプリケーションソフト／データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト／データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止することができる。第2の発明によれば、アプリケーションソフト／データを記録媒体に書き込んで各端末に配布するデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可／禁止するための書き込みを行うことで、端末毎のアクセス制御が可能となりセキュリティ維持と共に、アクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止することができる。第3の発明は、端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可することで、不法なアプリケーションソフト／データのダウンロードを禁止し、そのセキュリティを維持することができる。

#### 図の説明

##### 【図面の簡単な説明】

【図1】オフライン型のクライアント・サーバシステムを示したシステム構成図。

【図2】(A) 端末対応のCFカード3内のデータを示した図、(B) は端末グループA対応のCFカード3内のデータを示した図、(C) は端末グループB対応のCFカード3内のデータを示した図。

【図3】端末グループA、端末グループBを説明するための図。

【図4】(A) は端末登録テーブル7のデータ構造を示した図、(B) はアプリ・データ設定テーブル8のデータ構造を示した図、(C) はグループ登録テーブル9のデータ構造を示した図。

【図5】サーバコンピュータ1（携帯端末2）の全体構成を示したブロック図。

【図6】サーバコンピュータ1側の特徴的な動作を示したフローチャート。

【図7】携帯端末2側の特徴的な動作を示したフローチャート。

【図8】第2実施形態におけるオンライン型クライアント・サーバシステムを示したシステム構成図。

【図9】第2実施形態においてクライアント端末32側の動作を示したフローチャート。

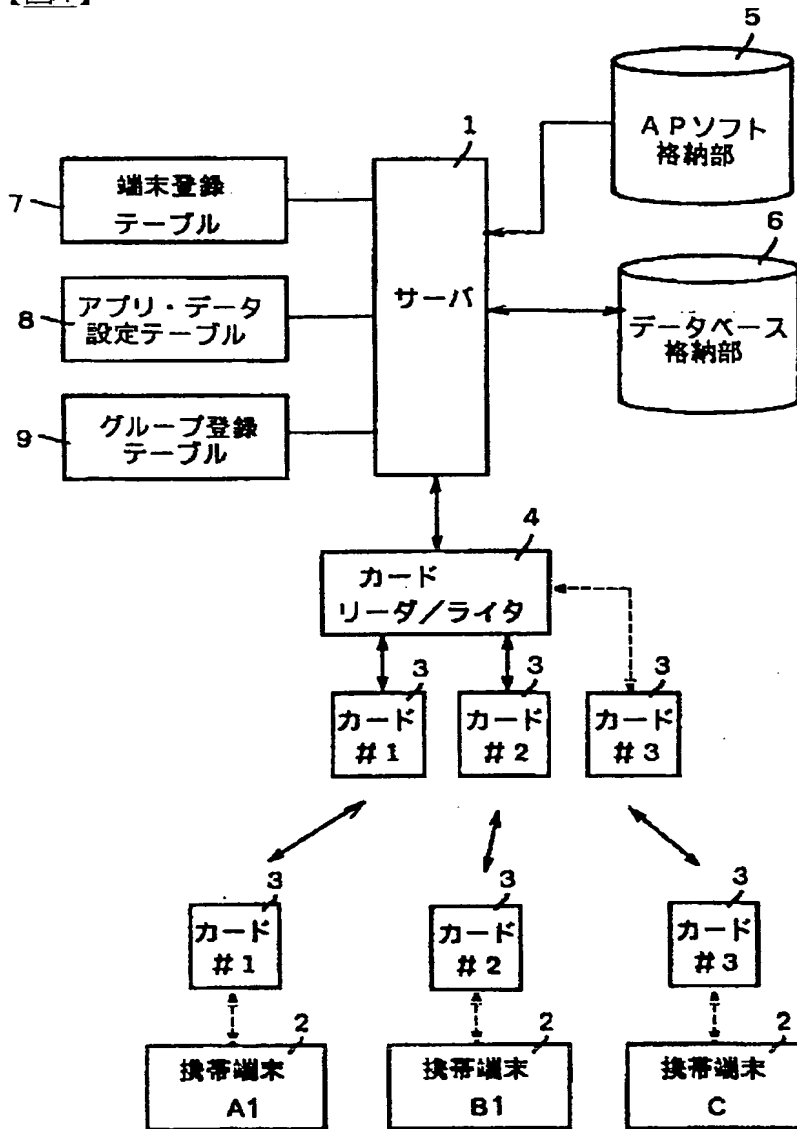
【図10】第2実施形態においてサーバコンピュータ31側の動作を示したフローチャート。

5 【符号の説明】

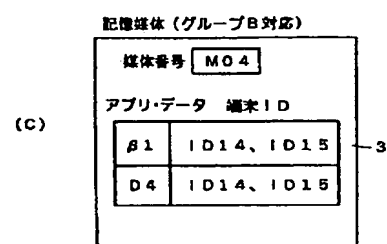
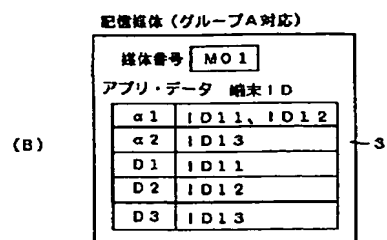
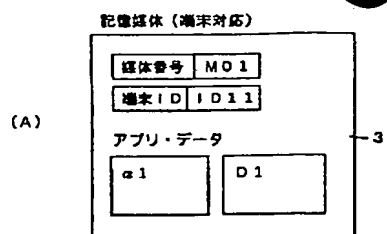
- 1、31 サーバコンピュータ
- 2 携帯端末
- 3 CFカード
- 4 カードリーダー/ライター
- 10 5 APソフト格納部
- 6 データベース格納部
- 7、33 端末登録テーブル
- 8、34 アプリ・データ設定テーブル
- 9 グループ登録テーブル
- 15 32 クライアント端末
- A、B 端末グループ

図面

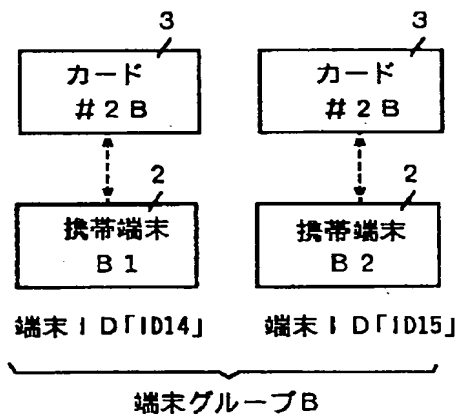
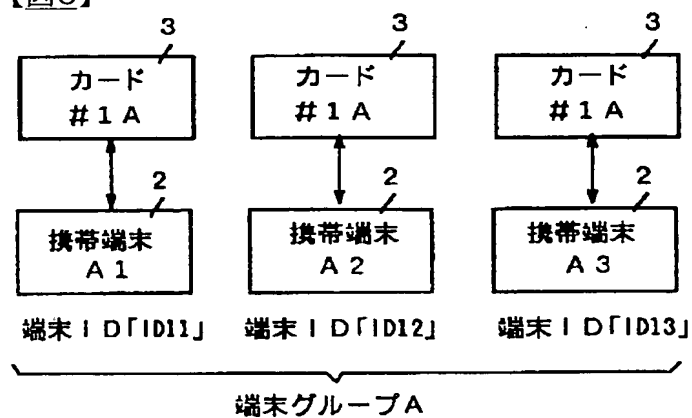
【図1】



【図2】



【図3】



【図4】

端末登録テーブル

(A)

端末名称	端末ID	媒体番号
A1	ID11	M01
A2	ID12	M02
A3	ID13	M03
B1	ID14	M04
B2	ID15	M05

アプリ、データ設定テーブル

(B)

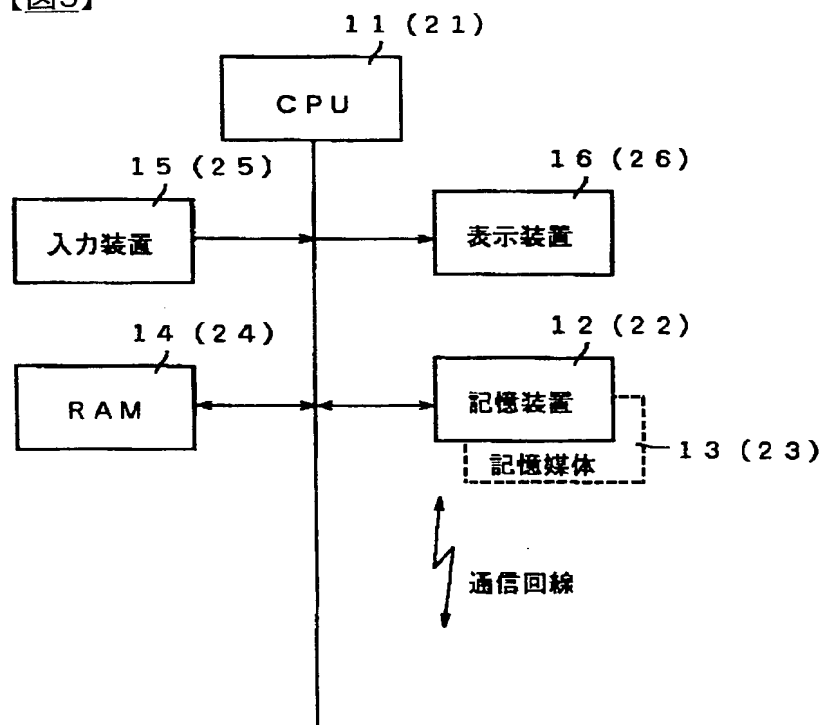
アプリデータ	端末ID	書き込みフラグ
アプリα1	ID11	
	ID12	
アプリα1	ID13	
アプリβ1	ID15	
	ID14	
データD1	ID11	
データD2	ID12	
データD3	ID13	
データD4	ID14	
	ID15	

グループ登録テーブル

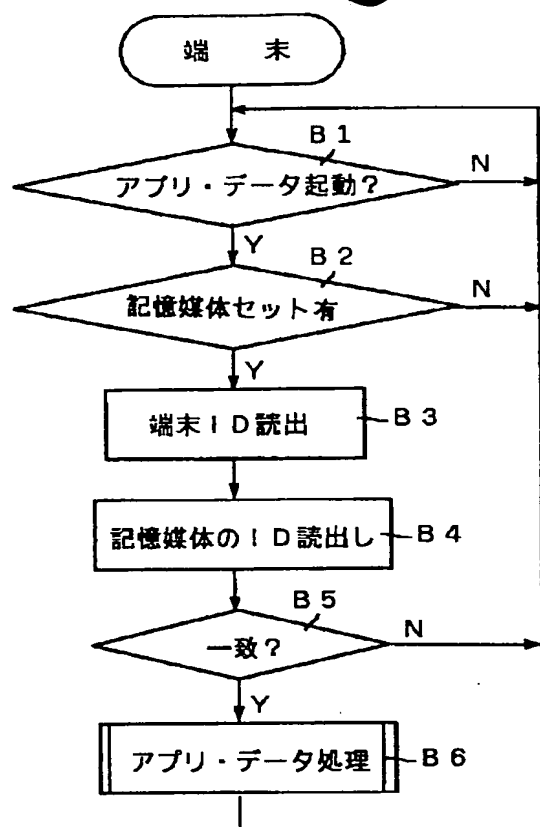
(C)

端末グループ名称	端末ID
A	ID11
	ID12
	ID13
B	ID14
	ID15

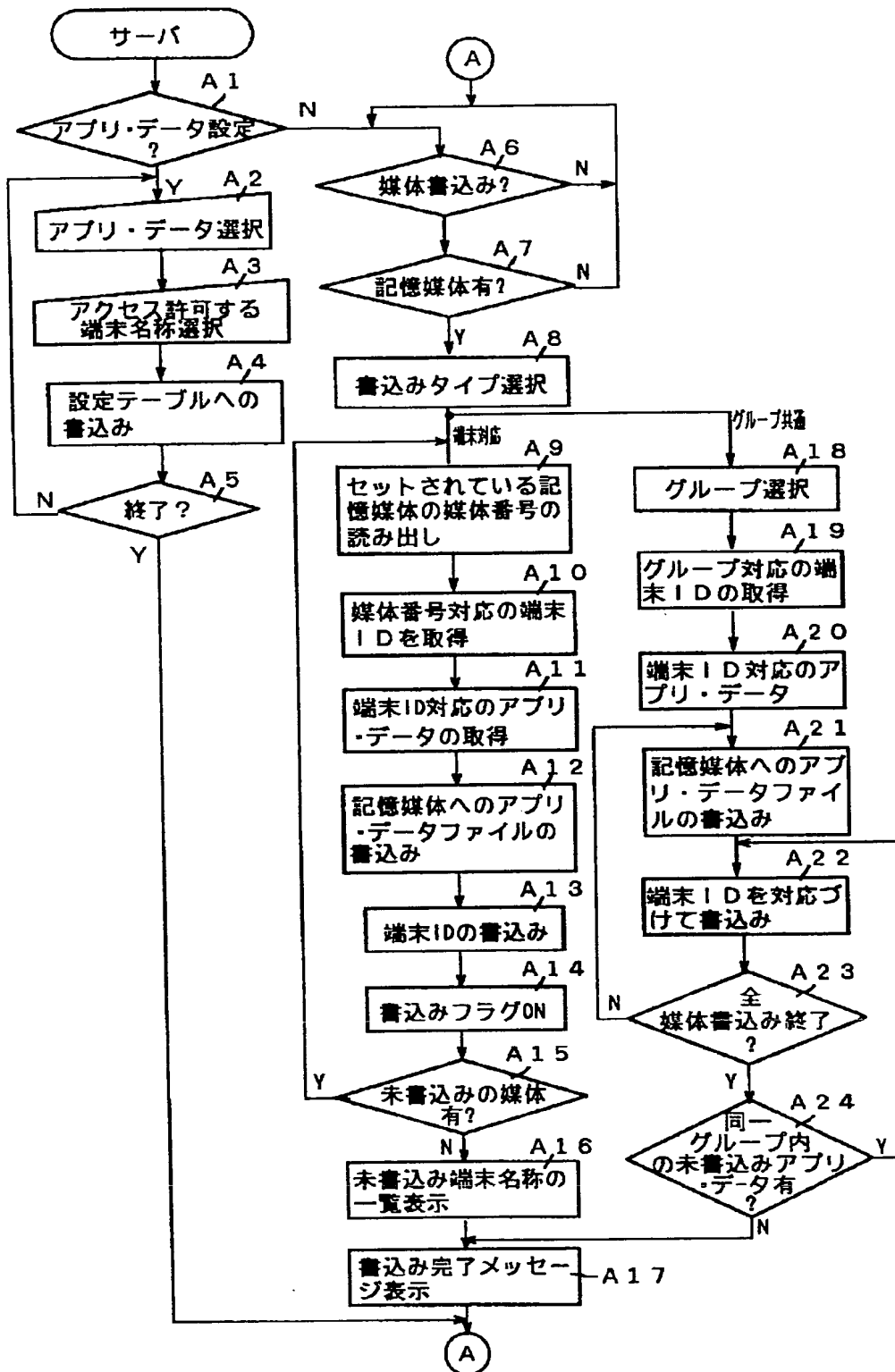
【図5】



【図7】

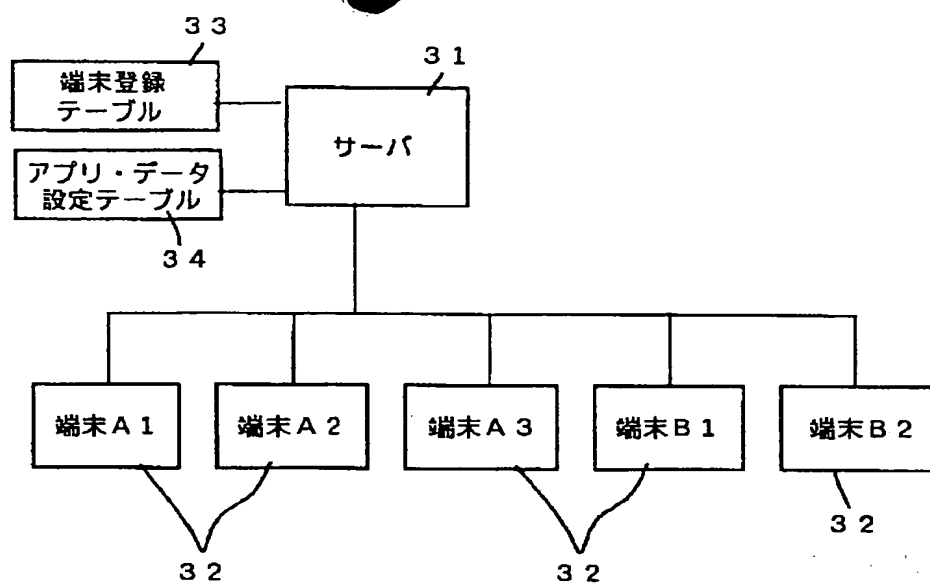


【図6】

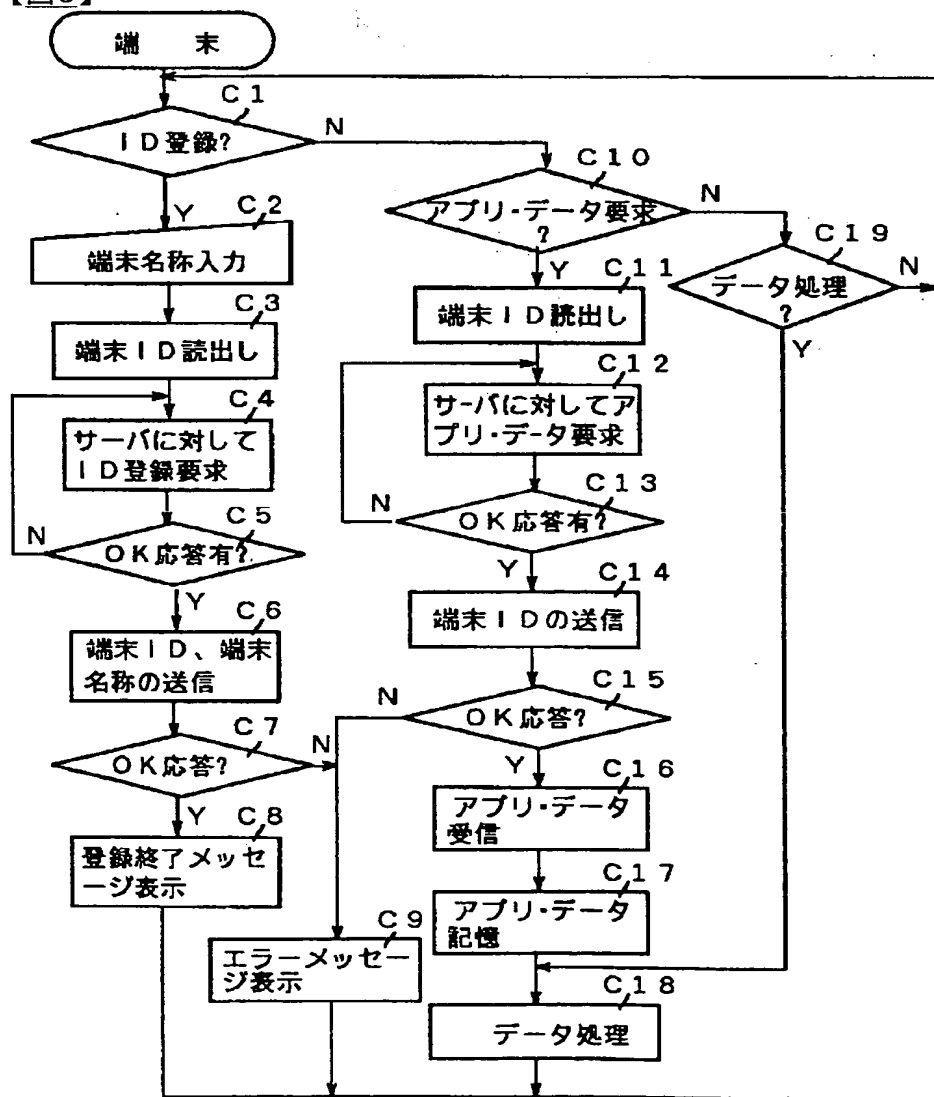


【図8】





【図9】



【図10】

